On the Beneficial Role of a Finite Number of Scatterers for Wireless Physical Layer Security

Espinosa, Pablo Ramirez; Sánchez-Alarón, José; López-Martínez, F. Javier

Published in:
IEEE Access

DOI (link to publication from Publisher):
10.1109/ACCESS.2020.2999719

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 1, 2020, accepted May 21, 2020, date of publication June 3, 2020, date of current version June 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2999719

On the Beneficial Role of a Finite Number of Scatterers for Wireless Physical Layer Security

PABLO RAMÍREZ-ESPINOSA[1], R. JOSÉ SÁNCHEZ-ALARCÓN[2], AND F. JAVIER LÓPEZ-MARTÍNEZ[2], (Senior Member, IEEE)

[1]Department of Electronic Systems, Connectivity Section, Aalborg University, 9220 Aalborg, Denmark
[2]Departamento de Ingenieria de Comunicaciones, Universidad de Malaga, 29071 Malaga, Spain

Corresponding author: Pablo Ramírez-Espinosa (pres@es.aau.dk)

This work was supported by the Spanish Government and the European Fund for Regional Development FEDER under Project TEC2017-87913-R and by Junta de Andalucia (Project P18-RT-3175, TETRA5G).

ABSTRACT We show that for a legitimate communication under multipath quasi-static fading with a reduced number of scatterers, it is possible to achieve perfect secrecy even in the presence of a passive eavesdropper for which no channel state information (CSI) is available. Specifically, we show that the outage probability of secrecy capacity (OPSC) is zero for a given range of average signal-to-noise ratios (SNRs) at the legitimate and eavesdropper's receivers. As an application example, we analyze the OPSC for the case of two scatterers, explicitly deriving the relationship between the average SNRs, the secrecy rate R_S and the fading model parameters required for achieving perfect secrecy. The impact of increasing the number of scatterers is also analyzed, showing that it is always possible to achieve perfect secrecy in this scenario, provided that (*i*) the dominant specular component for the legitimate channel is sufficiently large compared to the remaining scattered waves, and (*ii*) a exclusion area on which no eavesdroppers can be placed is considered.

INDEX TERMS Fading channels, outage probability, physical layer security, secrecy capacity.

I. INTRODUCTION

In the last decade, the seminal works in [1]–[3] have boosted the interest of the research community for providing secure communications over wireless channels from an information-theoretic viewpoint based on the classical work by Shannon [4]. Compared to the case in which fading is neglected [5], [6], the effect of random fluctuations due to fading turns out being beneficial in many cases: in the presence of fading, secure communications are possible even when the legitimate receiver experiences a lower average signal-to-noise ratio (SNR) than the eavesdropper [2], [3], since the transmitter can benefit from the instants when the instantaneous SNR at the legitimate receiver is above that of the eavesdropper. In other circumstances, the secrecy capacity under fading may be larger than its additive white Gaussian noise (AWGN) counterpart. In those cases in which channel state information (CSI) of the eavesdropper is unknown at the legitimate transmitter, these previous works [1]–[3] show that it is not possible to ensure *perfect secrecy* in wireless fading channels, and only a probabilistic measure is available through the outage probability of secrecy capacity (OPSC) [1].

The field of wireless physical layer security (PLS) has now become a rather mature field and numerous works have been devoted to characterize the key performance metrics under different propagation conditions: multiple-input multiple-output (MIMO) systems [7]–[9], satellite communications systems [10], vehicular communications [11], [12], correlated fading channels [13], relays systems [14], [15], ultra dense networks [16], machine-to-machine communications in Internet of things (IoT) contexts [17] and propagation over distinct fading conditions [18]–[20]; just to mention some relevant examples. All these aforementioned works consider state-of-the-art fading models like those in [1]–[3], which are based on the central limit theorem (CLT) assumption. This gives rise to the Rician and Rayleigh models, or generalizations of these [21]–[23]. The presence of a diffusely propagating component arising from the superposition of a sufficiently large number of non-dominant received waves is common to all these models. In a way, the CLT provides an approximate solution to the sum of random phase vectors, which is one of the key problems in communication theory [24]–[26].

The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh.

Nowadays, because of the new use cases of wireless systems under the umbrella of 5G and its evolutions, there are several examples in which the propagation conditions may be substantially different to those predicted by state-of-the-art fading models. For instance, in mmWave communications, a scarce number of multipath components arrives at the receiver [27], so that diffuse scattering only becomes relevant when non-line-of-sight (NLoS) conditions are considered [28]. In a different context, the potential of large-intelligent surfaces (LIS) — also, reconfigurable intelligent surfaces (RIS) — [29]–[32] to design the amplitude and phases of the scattered waves in order to optimize system performance can also be translated into a superposition of a finite number of individual waves.

Due to the great deal of attention received by these aforementioned emerging scenarios, we revisit in this work the issue of secure communications over wireless channels, with one key question in mind: *What's the effect of considering a finite number of scatterers*[1] *on wireless physical layer security?* For the first time in the literature, and thanks to the fine-grain characterization of the wireless propagation captured by ray-based models, we demonstrate that it is possible to achieve *perfect secrecy* in the communication between two legitimate peers under multipath quasi-static fading, i.e., *zero* OPSC, as the number of scatterers is reduced. Since all previous CLT-based analyses indicated that perfect secrecy was not possible in wireless channels, we proved that this was an artifact caused by the consideration of having an infinite number of multipath waves arriving at the receiver ends. We determine the conditions under which perfect secrecy can be ensured, and then we give some practical examples using a ray-based fading model with an increasing number of multipath waves. We also observe that using the alternative definition of OPSC in [34], which, in contrast to those in [1]–[3], only accounts for outage events that actually compromise the security of the communication, secrecy performance can be further improved.

The remainder of this paper is structured as follows. The system model for PLS over fading channels with a finite number of rays is formulated in Section II. Then, the notion of perfect secrecy over ray-based fading channels is introduced in Section III. As an illustrative example, the two-ray case is analyzed in Sections IV and V, showing how secure and reliable transmission can be attained. The effect of considering a larger number of rays is analyzed in Section VI, whereas main conclusions are drawn in Section VII.

II. PROBLEM FORMULATION

A. SYSTEM MODEL FOR PLS

We consider a legitimate user (Alice) who wants to send confidential messages to another user (Bob) in the presence of an eavesdropper (Eve). For simplicity, yet without loss of generality, all these agents are equipped with single-antenna devices. The complex channel gains from Alice to Bob and Eve are denoted by h_b and h_e, respectively, and assumed constant during the transmission of an entire codeword but independent from one codeword to the next one, i.e., we consider quasi-static fading channels. Therefore, the instantaneous SNRs at Bob and Eve are given by

$$\gamma_b = \overline{\gamma}_b \frac{\|h_b\|^2}{\mathbb{E}[\|h_b\|^2]}, \quad \gamma_e = \overline{\gamma}_e \frac{\|h_e\|^2}{\mathbb{E}[\|h_e\|^2]}, \tag{1}$$

where $\mathbb{E}[\cdot]$ is the expectation operator and $\overline{\gamma}_b$ and $\overline{\gamma}_e$ denote the average SNR at Bob and Eve, respectively.

If Alice has perfect knowledge of both Bob's and Eve's instantaneous CSI, perfect secrecy can be obtained by adapting the transmision rate, R_s, in those instants where $\gamma_b > \gamma_e$ [1], [3]. The secrecy capacity, i.e., the maximum transmission rate ensuring a secure communication between Alice and Bob, is obtained by leveraging the classical results over real Gaussian channels in [5], [6] to model complex ones, leading to[2]

$$C_s = [C_b - C_e]^+ = [\log(1+\gamma_b) - \log(1+\gamma_e)]^+, \tag{2}$$

where C_b and C_e are the capacities of Bob and Eve, respectively, and $[x]^+$ is the shorthand notation for $\max\{0, x\}$. Thus, for each channel realization, Alice would transmit at a rate $R_s \leq C_s$ in order to avoid any information leakage to Eve.

Consider now a more realistic case in which Eve's instantaneous CSI is unknown at the transmitter (corresponding, e.g., to that of a purely passive eavesdropper). In this case, previous works state that perfect secrecy cannot be achieved, and therefore they resort on outage analysis [1]–[3], [34]. That is, Alice would blindly establish a target transmission rate, R_s, relying on the assumption that the secrecy capacity of the channel is larger than R_s. If $C_s < R_s$, then an outage occurs and the security of the tranmission is compromised with some probability. The interest lies then in the analysis of the probability of this event, namely OPSC, and defined as [1], [34]

$$P_{\text{out}}(R_s) \triangleq P\{C_s < R_s\}. \tag{3}$$

However, all the aforementioned works [1]–[3], [7]–[20] consider that the channel gains and, consequently, γ_b and γ_e, are distributed according to classical fading models arising from the assumption of CLT or generalizations of them, which ultimately inherits the diffuse component present in these classical distribuions. As stated before, these models may not be suitable to characterize channel conditions in some emerging scenarios such as mmWave communications or propagation through LIS [27], [28].

B. CLT AND RAY-BASED FADING MODELS

Due to the multipath propagation, the complex based-band received signals at both Bob and Eve are written as the

[1] i.e., objects or surfaces in the propagation environment on which electromagnetic waves impinge. Specifically, our goal is to determine how individual multipath waves not originated from diffuse scattering [33] affect physical layer security.

[2] Unless specifically stated, all the logarithmic functions in this paper are base 2.

superposition of multiple waves arising from reflections and scattering as [21, eq. (1)]

$$h_k = \sum_{i=1}^{N_k} V_{i,k} e^{j\phi_{i,k}}, \tag{4}$$

where $k = b, e$ denotes indistinctly Bob's or Eve's channel, N_k denotes the number of multipath waves[3], $V_{i,k} \in \mathbb{R}^+$ their constant amplitudes and $\phi_{i,k}$ their phases, which are assumed to be statistically independent and uniformly distributed over $[0, 2\pi)$. Traditionally, the sum in (4) is split into two groups of waves as

$$h_k = \sum_{i=1}^{M_k} V_{i,k} e^{j\phi_{i,k}} + \sum_{i=1}^{P_k} \widehat{V}_{i,k} e^{j\theta_{i,k}} \tag{5}$$

where $\theta_{i,k}\ \forall\ i$ are also independent and uniformly distributed. Hence, the first sum represents the contribution of the M_k dominant or specular components, whilst the second one groups the contribution of non-specular or diffuse waves, where the power of each component is considerably lower. Thus, the dominant waves are associated with the line-of-sight (LoS) components, whereas the diffuse part represents the contribution of reflections and scattering. When P_k is sufficiently large, i.e., we have a rich multipath propagation, the diffuse component can be regarded as Gaussian because of the CLT, and therefore

$$h_k = \sum_{i=1}^{M_k} V_{i,k} e^{j\phi_{i,k}} + \sigma_{x,k} X_k + j\sigma_{y,k} Y_k \tag{6}$$

with $X_k, Y_k \sim \mathcal{N}(0, 1)$ and $\sigma_{x,k}, \sigma_{y,k} \in \mathbb{R}^+$.

Equation (6) is the basis for most popular fading models, and the widespread classical distributions arise depending on the value of the parameters M_k, $\sigma_{x,k}$ and $\sigma_{y,k}$. For instance, if $\sigma_{x,k} = \sigma_{y,k}$ and $M_k = 0$ we obtain the Rayleigh model, whilst $M_k = 1$ yields the Rice distribution and $M_k = 2$ reduces to the two-wave with diffuse power (TWDP) model [21].

In stark contrast with the previous works, which consider channel gains according to (6), in this work we will stick to the general formulation in (4) in order to explicitly account for the effect of considering a *finite* number of multipath waves on PLS.

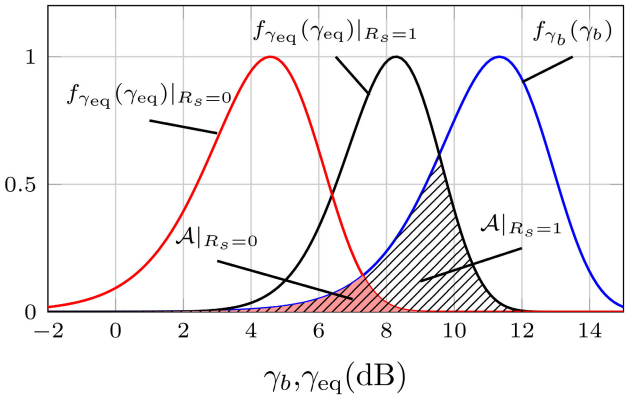
III. PERFECT SECRECY OVER FADING CHANNELS

A. IMPACT OF A REDUCED NUMBER OF SCATTERERS IN OPSC

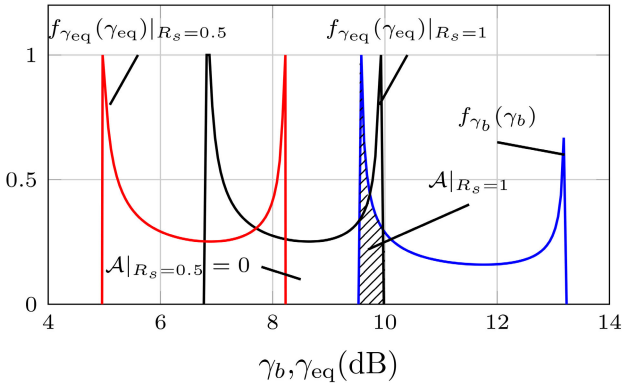
In order to better understand the influence of the fading distribution in the OPSC, we reformulate P_{out} in (3) in terms of Bob's and Eve's SNRs as

$$P_{\text{out}}(R_s) = P\{\gamma_b < 2^{R_s}\gamma_e + 2^{R_s} - 1\} = P\{\gamma_b < \gamma_{\text{eq}}\}, \tag{7}$$

[3]For a beautiful and complete formal description of ray-based models and their connection with the underlying electromagnetic theory, we gently refer the reader to [33].



(a) γ_b and γ_{eq} follow a fading distribution (Rician) arising from CLT.



(b) γ_b and γ_{eq} follow a ray-based fading distribution.

FIGURE 1. Common area under the PDFs of γ_b and γ_{eq} for classical and ray-based fading models, and different values of R_s ($\overline{\gamma_b} = 12$ dB and $\overline{\gamma_e} = 5$ dB). For better visualization, the PDFs in the figure have been normalized.

which is obtained by introducing (2) in (3) and performing some basic algebraic manipulations. Note that, when conditioning on γ_e, P_{out} corresponds to the cumulative distribution function (CDF) of γ_b and, therefore, it can be computed by averaging over all the possible states of γ_e as

$$P_{\text{out}}(R_s) = \int_0^\infty F_{\gamma_b}\left(2^{R_s}\gamma_e + 2^{R_s} - 1\right) f_{\gamma_e}(\gamma_e)\, d\gamma_e. \tag{8}$$

Regarding (7), it is clear that the condition for secrecy is $\gamma_b > \gamma_{\text{eq}}$, where γ_{eq} is obtained from γ_e as $\gamma_{\text{eq}} = 2^{R_s}\gamma_e + 2^{R_s} - 1$. From a geometric point of view, for a given value of γ_{eq}, the OPSC corresponds therefore to the area under the probability density function (PDF) of γ_b for which $\gamma_b < \gamma_{\text{eq}}$. If we consider the complete distribution of γ_{eq}, then the outage probability is related to the common area under the PDFs of γ_b and γ_{eq}, being the latter a rescaled and shifted version of $f_{\gamma_e}(\gamma_e)$ of the form

$$f_{\gamma_{\text{eq}}}(\gamma_{\text{eq}}) = 2^{-R_s} f_{\gamma_e}(2^{-R_s}(\gamma_{\text{eq}} + 1) - 1). \tag{9}$$

Thus, the larger this overlapped area in which γ_b can take lower values than γ_{eq}, the higher the outage probability. If we consider any fading distribution arising from the CLT assumption, i.e., the underlying random variables are Gaussian distributed, the PDFs of the SNRs – or, equivalently,

those of $\|h\|^2$ – are supported on a semi-infinite interval, and then the tails of $f_{\gamma_b}(\gamma_b)$ and $f_{\gamma_{\text{eq}}}(\gamma_{\text{eq}})$ overlap regardless of the values of R_s and the average SNRs. Hence, the condition of $\gamma_b < \gamma_{\text{eq}}$ is met with non-null probability and perfect secrecy cannot be achieved, as stated in [1]–[3], [34]. This can be observed in Fig. 1a, where even for $R_s = 0$ there exists some outage area, denoted by $\mathcal{A}$.

However, things are different when assuming ray-based fading models. Due to the consideration of a finite number of waves, there is a maximum and a minimum value for both the channel gains and the instantaneous SNRs, i.e., the PDFs of γ_b and γ_{eq} are supported on a bounded interval, say $[\gamma^{\min}, \gamma^{\max}]$. These limit values will depend on the relative amplitudes of the incident waves, that will add-up destructively/constructively with some probability. Therefore, it is evident that in some cases the distribution domains will be disjoint, and hence the OPSC can be identically zero, as showed in Fig. 1b. That is, under certain conditions, any possible value of γ_b will always be larger than γ_{eq}. This is an important observation, since it will allow us to achieve perfect secrecy for transmission rates $R_s > 0$ without Eve's CSI knowledge at the transmitter.

B. ACHIEVING PERFECT SECRECY OVER RAY-BASED FADING CHANNELS

Let us consider that the gains for both Eve's and Bob's channels are given by (4). For simplicity — yet without loss of generality — we assume that $V_{1,k} \geq V_{2,k} \geq \cdots \geq V_{N_k,k}$. It is clear that the maximum value of h_k, where $k = b, e$ is used again to distinguish between Bob's and Eve's gains, is obtained when all the waves in (4) are summed coherently. In turn, the minimum value arises when destructive combination occurs. Consequently, and in stark contrast with classical fading distributions, the domain of $\|h_k\|$ is bounded on the interval $[\|h_k^{\min}\|, \|h_k^{\max}\|]$ with

$$\|h_k^{\min}\| = \left[V_{1,k} - \sum_{i=2}^{N_k} V_{i,k} \right]^+, \quad \|h_k^{\max}\| = \sum_{i=1}^{N_k} V_{i,k}. \quad (10)$$

Therefore, this finite domain definition of channel gains allows us to achieve zero OPSC when a certain condition is met, as stated in the following proposition.

Proposition 1: Consider h_b and h_e as in (4). Then, for a given transmission rate $R_s > 0$, perfect secrecy, i.e., $P_{\text{out}}(R_s) = 0$, is achieved if

$$\gamma_b^{min} > 2^{R_s} \gamma_e^{max} + 2^{R_s} - 1, \quad (11)$$

where γ_b^{min} and γ_e^{max} are given by

$$\gamma_b^{min} = \overline{\gamma}_b \frac{\|h_b^{min}\|^2}{\mathbb{E}[\|h_b\|^2]}, \quad \gamma_e^{max} = \overline{\gamma}_e \frac{\|h_e^{max}\|^2}{\mathbb{E}[\|h_e\|^2]} \quad (12)$$

with $\|h_b^{min}\|$ and $\|h_e^{max}\|$ as in (10) and

$$\mathbb{E}[\|h_k\|^2] = \sum_{i=1}^{N_k} V_{i,k}^2, \quad k = b, e. \quad (13)$$

Proof: The condition for zero OPSC is given by $\gamma_b^{\min} > \gamma_{\text{eq}}^{\max}$. Since γ_{eq} is obtained as a linear transformation over γ_e, its maximum value occurs when $\gamma_e = \gamma_e^{\max}$, yielding immediately (11). On the other hand, (13) is obtained by calculating the expectation of the squared modulus of (4) and applying the multinomial theorem. ■

Inspecting (11), we observe that higher values of R_s imply a more restrictive perfect secrecy condition, i.e., if we aim to increase the transmission rate, we need $\gamma_b^{\min}$ to be larger. This is also shown in Fig. 1, where increasing R_s shifts $f_{\gamma_{\text{eq}}}$ to the right regardless of the considered fading distribution. Moreover, as $\overline{\gamma}_b$ becomes larger – or, equivalently, $\overline{\gamma}_e$ takes lower values – we can transmit at a faster secure rate while keeping zero OPSC, which is a coherent result.

We also observe that considering a larger number of rays in (4) has a significant impact in the OPSC. As N_k increases, either in Bob's or Eve's channel, the interval $[h_k^{\min}, h_k^{\max}]$ gets wider, causing the condition in (11) to be more restrictive. In fact, if $N \to \infty$, then (4) becomes a Gaussian random variable, rendering the classical fading distributions and implying that $\|h_k^{\min}\| \to 0$ and $\|h_k^{\max}\| \to \infty$, as predicted by CLT-based channel modeling approaches.

It is important to note that, although Eve's instantaneous CSI is not required, we implicitly make some assumptions regarding the distribution of h_e, i.e., the value of $\gamma_e^{\max}$, in order to apply the secrecy condition in (11). Because the relative amplitudes of the waves arriving at Eve as well as their average power are closely related to the geometry of the scenario under analysis, this is equivalent to assume that Alice has information over the propagation environment.

More specifically, some worst-case assumptions (equivalent to having statistical knowledge of CSI without explicitly requiring it) can be taken and still ensure perfect secrecy. For instance, an upper bound for the average SNR at Eve ($\overline{\gamma}_e$) can be determined by establishing exclusion areas (or secure areas) around the transmitter in which no eavesdroppers can be placed [35]. With the radius of the secure area, it is possible to calculate the minimum pathloss to Eve and therefore we can upper bound its average SNR. Note that the use of exclusion areas is usual in the related literature (see, e.g., [36], [37]). Similarly, the number of rays arriving at the eavesdropper can be designed from the geometry of the propagation scenario in case of highly directional transmissions, or by properly controlling the propagation environment using, e.g., large intelligent surfaces, which allow to modify at will the phases of the incident waves [29]–[32]. Thus, although technically no CSI may be available for a purely passive eavesdropper, we can still design the transmission in order to ensure perfect secrecy.

IV. SECURE TX OVER TWO-WAVE FADING

After formulating the conditions on which perfect secrecy can be attained when considering ray-based fading channels, we now analyze a simple, albeit illustrative, case by assuming two dominant components arriving at both receiver ends. The two-wave (or two ray) fading model [21], [38] arises when

setting $N_k = 2$ in (4), i.e.

$$h_k = V_{1,k}e^{j\phi_{1,k}} + V_{2,k}e^{j\phi_{2,k}}. \tag{14}$$

This model is completely characterized by the parameter

$$\Delta_k = \frac{2V_{1,k}V_{2,k}}{V_{1,k}^2 + V_{2,k}^2}, \tag{15}$$

which measures the relative difference in amplitude between the two waves. Hence, $\Delta_k = 1$ implies that both rays have exactly the same power, whilst $\Delta_k = 0$ signifies that one of the specular components in (14) vanishes.

With this consideration, the PDF and the CDF of the SNR at Bob and Eve are written as [21], [39]

$$f_{\gamma_k}^{\text{tw}}(\gamma_k) = \frac{1}{\pi\overline{\gamma}_k\sqrt{\Delta_k^2 - (1-\gamma_k/\overline{\gamma}_k)^2}} \quad \gamma_k^{\min} \le \gamma_k \le \gamma_k^{\max}, \tag{16}$$

$$F_{\gamma_k}^{\text{tw}}(\gamma_k) = \frac{1}{2} - \frac{1}{\pi}\text{asin}\left(\frac{1-\gamma_k/\overline{\gamma}_k}{\Delta_k}\right) \tag{17}$$

where, as in the previous section, the subindex $k = b, e$ is used to distinguish between the parameters of Bob's and Eve's channel distributions. The domain boundaries for each distribution are calculated as in (12), yielding in this case

$$\gamma_k^{\min} = \overline{\gamma}_k(1-\Delta_k), \quad \gamma_k^{\max} = \overline{\gamma}_k(1+\Delta_k), \tag{18}$$

and therefore the condition for perfect secrecy stated in Proposition 1 is expressed as

$$\overline{\gamma}_b > \frac{2^{R_s}\overline{\gamma}_e(1+\Delta_e) + 2^{R_s} - 1}{1-\Delta_b}. \tag{19}$$

Thus, despite the fact that Eve's instantaneous CSI is unkown at Alice, secrecy in the communication can be ensured if the average SNR at Bob is above a certain threshold. In case Alice does not have any statistical knowledge of Eve's channel, the transmission rate can be adapted based on the worst-case in which $\Delta_e = 1$. As previously indicated, when the average SNR at Eve is unknown, it can be upper-bounded by defining exclusion areas in which no eavesdroppers are possible. Hence, even in this situation, the perfect secrecy condition can be met, e.g., by a proper design of the distance between the transmitter and the legitimate receiver. After simple manipulations to (19), the largest constant rate that ensures perfect secrecy is expressed as

$$R_s^{\max} = \left[\log\left(\frac{\overline{\gamma}_b(1-\Delta_b)+1}{\overline{\gamma}_e(1+\Delta_e)+1}\right)\right]^+. \tag{20}$$

In fact, whenever Alice has perfect knowledge of Bob's CSI (instead of statistical knowledge only), it is possible to adapt its transmission rate to Bob's instantaneous CSI while meeting the condition $\gamma_b > \overline{\gamma}_e(1+\Delta_e)$, which yields the following expression for the instantaneous secrecy capacity:

$$C_s = \left[\log\left(\frac{\gamma_b+1}{\overline{\gamma}_e(1+\Delta_e)+1}\right)\right]^+ \ge R_s^{\max}. \tag{21}$$

The OPSC over two-wave fading is straightforwardly calculated by introducing (16) and (17) in (8), leading to

$$P_{\text{out}}^{\text{tw}}(R_s) = \frac{1}{\pi\overline{\gamma}_e}\int_{\gamma_e^{\min}}^{\gamma_e^{\max}} \frac{\widehat{F}_{\gamma_b}^{\text{tw}}\left(2^{R_s}\gamma_e + 2^{R_s} - 1\right)}{\sqrt{\Delta_e^2 - (1-\gamma_e/\overline{\gamma}_e)^2}}\, d\gamma_e \tag{22}$$

with

$$\widehat{F}_{\gamma_k}^{\text{tw}}(\gamma) = \begin{cases} 0, & \text{if } \gamma < \gamma_k^{\min} \\ \frac{1}{2} - \frac{1}{\pi}\text{asin}\left(\frac{1-\gamma/\overline{\gamma}_k}{\Delta_k}\right), & \text{if } \gamma_k^{\min} < \gamma < \gamma_k^{\max} \\ 1, & \text{if } \gamma > \gamma_k^{\max}, \end{cases} \tag{23}$$

where the piecewise definition of $\widehat{F}_{\gamma_k}^{\text{tw}}(\gamma)$ is a consequence of the finite domain of $F_{\gamma_k}^{\text{tw}}(\gamma_k)$ in (17).

A simple and accurate approximation for the OPSC in (22) can be obtained by applying quadrature methods. Note that the integrand presents a singularity at $\gamma_e = \gamma_e^{\max}$, and thus we must carefully choose the weights of the quadrature approximation. Since the singularity is of the type $(1-x^2)^{-1/2}$, Chebyshev-Gauss' method is the more appropriate [40, eq. eq. (25.4.38)]. Therefore, by performing the change of variables $(1-\gamma_e/\overline{\gamma}_e)/\Delta_e = x$ and applying the aforementioned quadrature technique, the outage probability is approximated as

$$P_{\text{out}}^{\text{tw}}(R_s) \approx \frac{1}{n}\sum_{i=1}^{n}\widehat{F}_{\gamma_b}^{\text{tw}}\Bigg(2^{R_s} - 1 + 2^{R_s}\overline{\gamma}_e\left[1 - \Delta_e\cos\left(\frac{(2i-1)\pi}{2n}\right)\right]\Bigg), \tag{24}$$

where n is the approximation order, reducing the integral to a finite sum of evaluations of $F_{\gamma_b}^{\text{tw}}(\cdot)$. In most cases, (24) provides accurate approximations even for relatively low values of n, e.g., $n = 10$, and it is faster to compute than (22). Note, however, than (22) can also be computed without difficulties using standard calculation software such as Matlab or Mathematica.

The outage probability in (22) in terms of R_s and $\overline{\gamma}_b$ is depicted in Figs. 2 and 3, respectively. For the sake of comparison, P_{out} over CLT based channels (in this case, Rayleigh fading) is also shown as a reference. We observe that, for a given $R_s < R_s^{\max}$, the outage probability is exactly zero when considering a finite number of reflections, whilst this behavior is not reproduced when assuming a fading model arising from the CLT. Specifically, we observe that the asymptotic decay for the Rayleigh case (i.e., the negative slope of the OPSC as $\overline{\gamma}_b$ grows) is that of a diversity order equal to one. Conversely, when considering the ray-based alternatives here analyzed the OPSC abrutly drops for the limit value of $\overline{\gamma}_b$ given by (18), which can be regarded as an *infinite* diversity order. As $\Delta_b \to 1$, we see from (19) that $\gamma_b^{\min} \to 0$ and hence perfect secrecy cannot be achieved for operational values of $\overline{\gamma}_b$. Interestingly, the asymptotic decay for this particular configuration on which $\Delta_b = 1$ is that

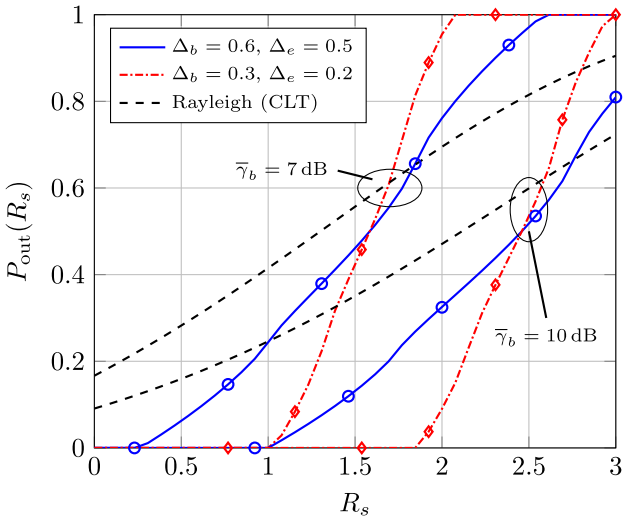


FIGURE 2. Impact of CLT based fading models (Rayleigh) and ray-based ones (Two-wave) in the OPSC for different values of channel parameters and average SNRs. For all traces, $\overline{\gamma}_e = 0$ dB. Solid lines correspond to theoretical calculations whilst markers correspond to MC simulations.

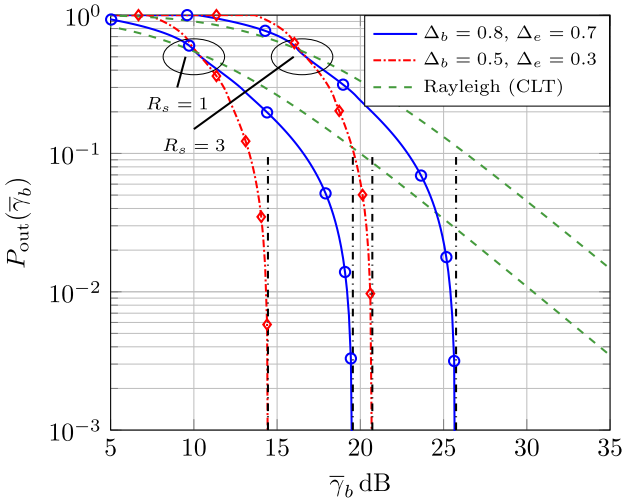


FIGURE 3. OPSC in terms of $\overline{\gamma}_b$ for different values of channel parameters and distinct fading models. For all traces $\overline{\gamma}_e = 7$ dB. Solid lines correspond to theoretical calculations whilst markers correspond to MC simulations. Dashdotted vertical lines correspond to the asymptotic OPSC.

of a diversity order equal to 1/2 [39] i.e., lower than in the Rayleigh case, as shown in Fig. 4.

We also notice that the parameter Δ_k plays an important role in the OPSC; as Δ_k increases, i.e., the power of the rays becomes more similar in either Bob's or Eve's channels, $R_s^{\max}$ takes lower values. Then, larger values of Δ_k render a lower achievable transmission rate or, equivalently, require higher values of the average SNR at Bob for the same R_s. It is interesting to pay attention to the limit values of both Δ_e

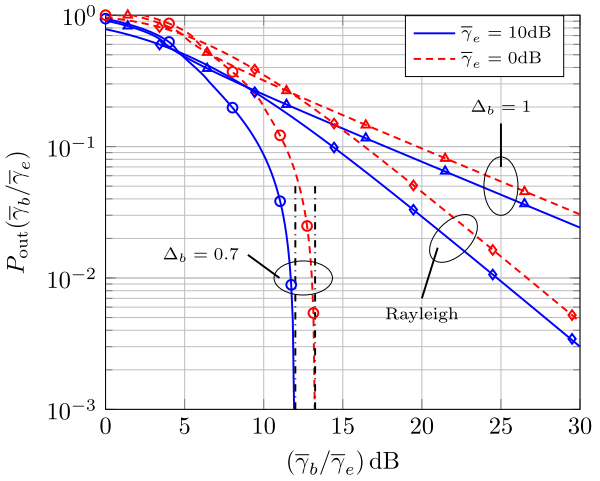


FIGURE 4. OPSC in terms of the ratio $\overline{\gamma}_b/\overline{\gamma}_b$ for different channel conditions and distinct values of channel parameters and average SNRs. For all traces, $R_s = 1.5$. Solid lines correspond to theoretical calculations whilst markers correspond to MC simulations. Dashdotted vertical lines correspond to the asymptotic OPSC.

and Δ_b. While setting $\Delta_e = 1$ still allows to achieve perfect secrecy, substituting $\Delta_b = 1$ in (20) makes $R_s^{\max} = 0$, as stated before.

Finally, it is important to note that the OPSC does not only depend on the relative values between $\overline{\gamma}_b$ and $\overline{\gamma}_e$, but also on the absolute ones. This is clearly observed from the perfect secrecy condition in (11) by dividing both terms of the inequality by $\overline{\gamma}_e$. Specifically, the value of $\overline{\gamma}_b/\overline{\gamma}_e$ required to achieve perfect secrecy decreases as $\overline{\gamma}_e$ increases, as shown in Fig. 4, where fixing $\overline{\gamma}_e = 10\,dB$ renders lower outage probabilities than the case $\overline{\gamma}_e = 0\,dB$ for the same ratio $\overline{\gamma}_b/\overline{\gamma}_e$.

V. SECURE AND RELIABLE TX OVER TWO-RAY FADING

Up to this point, we have considered the classical definition of OPSC given in (3). However, this formulation does not distinguish between outage events produced by a failure in achieving perfect secrecy ($R_s > C_s$) or due to the fact that Bob cannot decode the transmitted message (e.g., because its instantaneous SNR drops below the minimum value required for a reliable communication) [34]. Therefore, we revisit the outage formulation in [34, Sec. III], according to which the OPSC is defined as

$$P_{\text{out}}(R_s) \triangleq P\{R_s > C_b - C_e \,|\, \gamma_b > \gamma_{\text{th}}\} \tag{25}$$

where $\gamma_{\text{th}} \geq 0$ is the minimum SNR at Bob required for a reliable communication. Because Bob is supposed to collaborate with Alice, then the latter can suspend the transmission if $\gamma_b < \gamma_{\text{th}}$, since it would make no sense transmitting when the legitimate receiver cannot decode the message. With

$$P_{\text{out}}(R_s) = \frac{1}{1 - F_{\gamma_b}(\gamma_{\text{th}})}\left[\int_{\left[\frac{\gamma_{\text{th}}+1}{2^{R_s}}-1\right]^+}^{\infty} F_{\gamma_b}\left(2^{R_s}\gamma_e + 2^{R_s} - 1\right) f_{\gamma_e}(\gamma_e)\, d\gamma_e\right] - \frac{F_{\gamma_b}(\gamma_{\text{th}})\left[1 - F_{\gamma_e}\left(\frac{\gamma_{\text{th}}+1}{2^{R_s}} - 1\right)\right]}{1 - F_{\gamma_b}(\gamma_{\text{th}})}. \tag{26}$$

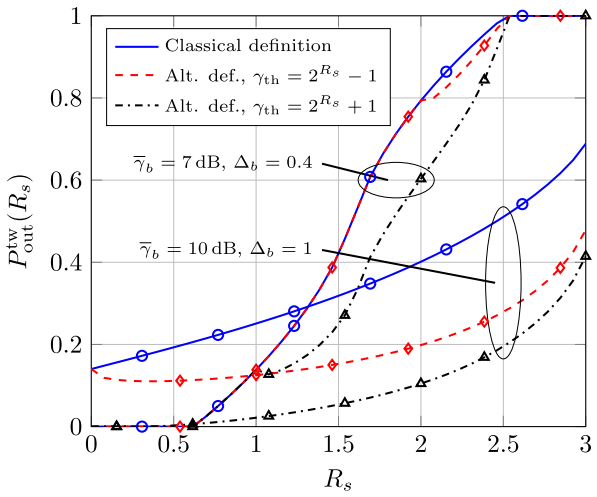


FIGURE 5. Comparison between classical and alternative OPSC formulation for different values of channel parameters and distinct SNR thresholds. For all traces, $\overline{\gamma}_e = 0$ dB and $\Delta_e = 0.6$. Solid lines correspond to theoretical calculations whilst markers correspond to MC simulations.

the OPSC definition in (3), this situation would produce an outage but, in fact, secrecy is not compromised since there would not be any message transmission.

Therefore, introducing (2) in (25), P_{out} is rewritten as

$$P_{\text{out}}(R_s) = \frac{P\left\{\gamma_{\text{th}} < \gamma_b < 2^{R_s}\gamma_e + 2^{R_s} - 1\right\}}{P\{\gamma_b > \gamma_{\text{th}}\}}, \qquad (27)$$

which, after some algebraic manipulations, leads to (26) (see Appendix A), placed at the bottom of the previous page. Note that (26) is valid for any arbitrary fading distribution, and not only for ray-based models. In fact, specializing for the Rayleigh distribution, (26) becomes [34, eq. (7)]. We can also observe that, if $\gamma_{\text{th}} = 0$, then (27) becomes (7), since we eliminate any reliability constraint.

Consider again the case of a finite number of reflections arriving to the receiver, i.e., the channel gains follow a ray-based distribution as in (4). Coming back to the geometrical meaning of the OPSC, conditioning P_{out} to the transmission event is equivalent to truncating the left tail of $f_{\gamma_b}(\gamma_b)$ in Fig. 1. Hence, the perfect secrecy condition is now formulated as

$$\max\{\gamma_b^{\min}, \gamma_{\text{th}}\} > 2^{R_s}\gamma_e^{\max} + 2^{R_s} - 1, \qquad (28)$$

with $\gamma_b^{\min}$ and $\gamma_e^{\max}$ given in (12). Note that the condition is less restrictive than that in Proposition 1, allowing us to achieve perfect secrecy in those scenarios where $\gamma_b^{\min}$ takes lower values, i.e., $\gamma_b^{\min} \to 0$. Thus, by properly choosing γ_{th}, it is possible to ensure secrecy at the expense of a lower transmission probability, which ultimately translates into a reduced throughput.

This is represented in Fig. 5, where the classical (3) and the alternative (25) definitions of OPSC are compared. The channels gains are assumed to follow a two-wave distribution, and therefore $P_{\text{out}}^{\text{tw}}$ is calculated by substituting (16) and (17) in (26) and taking into account the boundaries of $F_{\gamma_k}(\gamma_k)$.

Let us first consider the case on which $\overline{\gamma}_b = 7$ dB and $\Delta_b = 0.4$. We observe that, until R_s reaches a certain value, $\gamma_{\text{th}} < \gamma_b^{\min}$ and thus the transmission condition has no impact on the OPSC, since it is always met. Naturally, as the threshold increases, such limit value for R_s is reduced.

Regard now the case with $\overline{\gamma}_b = 10$ dB and $\Delta_b = 1$. As stated before, by choosing a sufficiently large threshold value γ_{th}, we can ensure perfect secrecy even when $\Delta_b = 1$ (or, equivalently, $\gamma_b^{\min} = 0$). However, increasing γ_{th} implies a lower throughput, given by $\eta = P\{\gamma_b > \gamma_{\text{th}}\}R_s$.

VI. IMPACT OF THE NUMBER OF SCATTERERS

In the previous sections, we have assumed a two-wave distribution for both Bob's and Eve's channel, i.e., $N_k = 2$ in (4). Due to the clear impact of N_k in the perfect secrecy condition stated in Proposition 1, we are now interested in analyzing the consequences of having a larger number of reflections arriving at the receiver. Specifically, two theoretical scenarios are considered: (i) *fixed average receive power and different number of scatterers* and (ii) *number of scatterers as a design parameter*.

A. FIXED AVERAGE SNR AND DIFFERENT N

In this situation, an increased number of reflectors and scatterers renders a richer multipath propagation and, consequently, larger values of both N_b and N_e, with N_b and N_e denoting the number of rays in (4) for Bob's and Eve's channels, respectively. Hence, for some given $\overline{\gamma}_b$ and $\overline{\gamma}_e$, our goal is to determine the what extent the consideration of a larger N_b and N_e impacts the secrecy performance. Since the limit case of $\{N_b, N_e\} \to \infty$ reduces to the Rayleigh fading case, we expect that the perfect secrecy condition in Proposition 1 is not met beyond some limit values of $\{N_b, N_e\}$.

We now express h_b and h_e as

$$h_k = V_{1,k}e^{j\phi_{1,k}} + \sum_{i=2}^{N_k} V_{i,k}e^{j\phi_{i,k}}, \quad k = e, b. \qquad (29)$$

with the amplitudes of the rays given by $V_{i,k} = \alpha_{i,k}V_{1,k}$ for $i = 2, \ldots, N_k$, with $0 < \alpha_{i,k} < 1$ and $\alpha_{i,k} \geq \alpha_{j,k}, \forall\, i < j$; i.e., the amplitude of the successive rays is expressed as relative to the amplitude of the dominant component.

For simplicity, and to better visualize the impact of increasing N, we consider again the classical outage formulation in (7). Therefore, it is clear that increasing the number of waves at reception makes the secrecy condition more restrictive. On the one hand, if N_b increases, then $\gamma_b^{\min}$, which directly depends on $\|h_b^{\min}\|$ in (10), takes lower values. On the other hand, $\gamma_e^{\max}$ also rises with N_e.

The effect of increasing the number of rays is studied in Fig. 6, where the OPSC is evaluated for different values of $N = N_b = N_e$. We also set $\alpha_{i,k} = \alpha$, which can be regarded as a worst case situation in terms of secrecy performance. Due to the mathematical complexity of the PDF of the ray-based model in (4) when $N > 3$, which involves the integral of

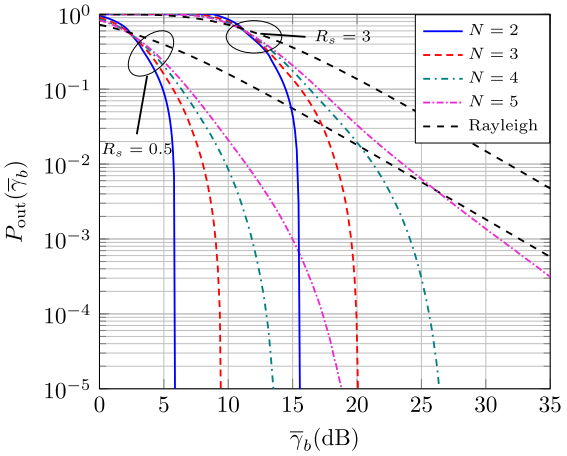


FIGURE 6. Impact of increasing the number of waves at both Eve and Bob. h_b and h_e are distributed according to (29) with $\alpha = 0.2$ for $R_s = 0.5$ and $\alpha = 0.25$ for $R_s = 3$. Also, $N_b = N_e = N$.

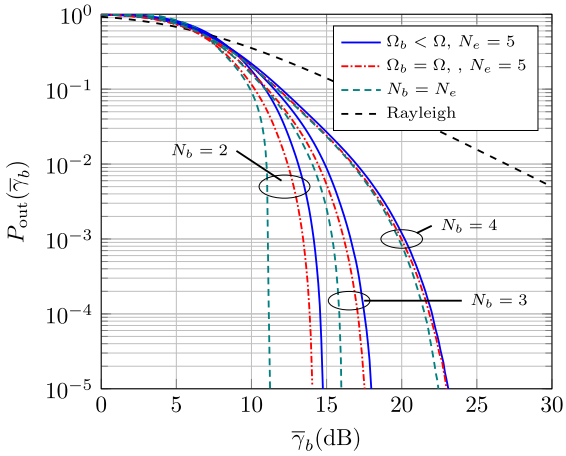


FIGURE 7. Impact of controlling the number of waves arriving at Bob. The wave amplitudes relation is given by (29) with $\alpha_{i,k} = \alpha = 0.2$. The case with power loss is compared with the theoretical case in which $\Omega_b = \Omega$ and with that where $N_e = N_b$. For all the traces R_s has been fixed to $R_s = 1$.

multiple Bessel's functions [41], we resort on Monte Carlo simulations for this section.

We observe in Fig. 6 that considering a larger number of waves requires higher values of $\overline{\gamma}_b$ to achieve the same outage probability, for a fixed R_s. Moreover, the average SNR at Bob needed to ensure perfect secrecy also changes with N, which is a coherent result since we are both reducing the value of $\gamma_b^{\min}$ and increasing $\gamma_e^{\max}$. Note that the relation between the amplitudes V_i also plays a key role on achieving perfect secrecy. For instance, in the case $R_s = 3$, in which $\alpha = 0.25$, we cannot ensure a secure transmission for $N = 5$, in contrast to the case $R_s = 0.5$ and $\alpha = 0.2$. This is explained as follows: since we need $\gamma_b^{\min} > \gamma_e^{\max}$, this translates into

$$V_{1,b} - \sum_{i=2}^{N_b} V_{i,b} > 0. \tag{30}$$

Thus, considering the relation between amplitudes as in (29), we have that $\alpha(N_b - 1) < 1$. Hence, if $\alpha = 0.25$ and $N = 5$, the condition is not met and therefore no perfect secrecy can be ensured in this case.

B. DESIGNING N FOR SECRECY

Let us now move into the second scenario, in which we assume that we are able to control the number of waves arriving at the receiver ends, i.e., we can somehow *eliminate* some of the rays by a proper design of the propagation characteristics of the environment. To that end, the use of LIS and RIS arises as a promising solution, since the phases of the incident waves at each surface can be deliberately modified [29]–[31]. Therefore, we could intentionally avoid that certain rays arrive the receiver.

This has, obviously, a non-negligible impact on the receiver power, since we are disregarding some components of the channel and hence diminishing its average power. This approach seems desirable for the eavesdropper channel, in the sense that it degrades its average SNR. However, since CSI needs to be known in order to properly configure the intelligent surfaces, we here consider the more realistic case in which we can only manipulate the number of waves arriving at the legitimate user, Bob, which is supposed to collaborate with Alice. As we will later see, and despite being somehow counterintuitive, reducing the number of rays also turns out being beneficial for the legitimate channel even though we are effectively decreasing the average SNR at Bob. For this reason, we will specialize our study on the consideration of a fixed number of rays for the eavesdropper channel, and a successive reduction on the number of rays received by Bob.

In order to characterize the SNR loss incurred by Bob, we consider the SNRs at both Bob and Eve given by

$$\gamma_b = \overline{\gamma}_b \frac{\|h_b\|^2}{\Omega}, \quad \gamma_e = \overline{\gamma}_e \frac{\|h_e\|^2}{\Omega}, \tag{31}$$

where h_e and h_b are given as in (4) with $N_e = N$ and $N_b < N$, representing the reduced number of waves arriving at Bob. The power loss is characterized by normalizing both channels by[4] $\Omega = \sum_{i=1}^{N} V_i^2$. Thus, $\mathbb{E}[\|h_b\|^2]/\Omega < 1$, which is equivalent to scale $\overline{\gamma}_b$ by a factor $\mathbb{E}[\|h_b\|^2]/\Omega = \Omega_b/\Omega$.

With this consideration, the OPSC is plotted in Fig. 7 for different values of N_b but maintaining the number of waves at Eve. For the sake of comparison, we also include the case of the first scenario in which $N_b = N_e$ and $\Omega_b = \Omega$ and the case $\Omega_b = \Omega$ but $N_b < N_e$. We observe that, despite the fact that Bob's average SNR is lowered, having a reduced number of waves arriving at Bob is beneficial from a secrecy perspective. Note that the impact of eliminating rays on the legitimate channel (and therefore having a lower received power) is less detrimental as N_b approaches N_e. In fact, considering h_k as in (29) with $\alpha_{i,k} = \alpha\ \forall\ i$ and $k = b, e$, the power loss can be written as

$$\frac{\Omega_b}{\Omega} = \frac{1 + \alpha^2(N_b - 1)}{1 + \alpha^2(N_e - 1)}. \tag{32}$$

[4]Note that we are assuming $V_{i,b} = V_{i,e}\ \forall\ i$.

Then, from (32), it is clear that such loss reduces as N_b increases, being equal to one if $N_b = N_e$, i.e., if we do not *eliminate* any ray.

Finally, we also note that the most favorable case is that where both Bob and Eve receive a small number of waves, which confirms the beneficial role of a reduced number of scatterers for wireless physical layer security.

VII. CONCLUSION

In this work, we provided a new look at wireless PLS, backing off from the classical CLT assumption associated to fading and explicitly accounting for the effect of considering a finite number of multipath waves arriving the receiver ends. To the best of our knowledge, we showed for the first time that it is possible to achieve *perfect secrecy* even when the eavesdropper's CSI is unknown at the transmitter.

We also showed that a rich multipath propagation (i.e., either a large number of specular reflections, the presence of diffuse scatterers that generate numerous multipath waves, or the consideration of double-bounce effects) has a negative impact on the OPSC, so that those propagation conditions, which imply a reduced number of waves arriving at the receiver ends, are instrumental to achieving perfect secrecy. Specifically, under ray-based propagation conditions, we proved that perfect secrecy can be achieved if the average SNR at the receiver is above a certain threshold, which depends on the number of rays present on each link and their relative amplitudes. This somehow contradicts the common knowledge that fading is beneficial for physical layer security; this assert is restricted to those situations on which the legitimate channel is more degraded that the eavesdropper's counterpart (and hence PLS is not possible in such case in the absence of fading), or when Eve's instantaneous CSI is available at Alice.

The consideration of a strong dominant specular component (i.e., larger than the remaining aggregate waves) is the key factor to enable perfect secrecy. We also showed that if the amplitudes of these remaining aggregate waves are equal or larger than that of the dominant component, then ray-based fading models are no longer beneficial from a secrecy point of view and the secrecy performance metrics obtained exhibit a similar behavior as those obtained through CLT approaches. Besides, incorporating a reliability constraint in the OPSC definition allows for improving the secrecy performance.

Finally, we also pointed out that the ability of controlling the propagation environment in order to reduce the number of waves arriving at the legitimate receiver is also beneficial for PLS. This opens up the possibility of using LIS to improve secrecy in a complete different way as those suggested in the literature, i.e., to eliminate reflections instead of for maximizing the SNR at Bob [42].

ACKNOWLEDGMENT

This article was presented in part at the XXXV URSI National Symposium [43].

APPENDIX A PROOF OF EQ. (26)

Conditioned on γ_e, (27) is written in terms of the CDF of γ_b as

$$P_{\text{out}}(R_s|\gamma_e) = \frac{F_{\gamma_b}\left(2^{R_s}\gamma_e + 2^{R_s} - 1\right) - F_{\gamma_b}(\gamma_{\text{th}})}{1 - F_{\gamma_b}(\gamma_{\text{th}})}. \tag{33}$$

In order to obtain the unconditioned outage probability, we need to average over all possible values of γ_e taking into account that, due to the reliability condition,

$$2^{R_s}\gamma_e + 2^{R_s} - 1 > \gamma_{\text{th}}. \tag{34}$$

Therefore, P_{out} is calculated as

$$P_{\text{out}}(R_s) = \int_{\left[\frac{\gamma_{\text{th}}+1}{2^{R_s}}-1\right]^+}^{\infty} P_{\text{out}}(R_s|\gamma_e) f_{\gamma_e}(\gamma_e)\, d\gamma_e, \tag{35}$$

where $f_{\gamma_e}(\gamma_e)$ is the PDF of Eve's SNR. Performing some algebraic manipulations to (35) immediately yields (26).

REFERENCES

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[3] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[7] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[8] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959–2971, Aug. 2015.

[9] X. Zhang, D. Guo, K. An, and B. Zhang, "Secure communications over cell-free massive MIMO networks with hardware impairments," *IEEE Syst. J.*, early access, Jun. 11, 2019, doi: 10.1109/JSYST.2019.2919584.

[10] K. Guo, K. An, B. Zhang, Y. Huang, X. Tang, G. Zheng, and T. A. Tsiftsis, "Physical layer security for multiuser satellite communication systems with threshold-based scheduling scheme," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5129–5141, May 2020.

[11] Y. Ai, M. Cheffena, A. Mathur, and H. Lei, "On physical layer security of double Rayleigh fading channels for vehicular communications," *IEEE Wireless Commun. Lett.*, vol. 7, no. 6, pp. 1038–1041, Dec. 2018.

[12] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, X. Li, and R. Kharel, "Physical layer security in vehicular networks with reconfigurable intelligent surfaces," 2019, *arXiv:1912.12183*. [Online]. Available: http://arxiv.org/abs/1912.12183

[13] X. Zhang, G. Pan, C. Tang, T. Li, and Y. Weng, "Performance analysis of physical layer security over independent/correlated log-normal fading channels," in *Proc. Australas. Telecommun. Netw. Appl. Conf. (ATNAC)*, Nov. 2014, pp. 23–27.

[14] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[15] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[16] M. Kamel, W. Hamouda, and A. Youssef, "Physical layer security in ultra-dense networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 5, pp. 690–693, Oct. 2017.
[17] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.
[18] L. Wang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247–258, Feb. 2014.
[19] H. Lei, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "Secrecy capacity analysis over α-μ fading channels," *IEEE Commun. Lett.*, vol. 21, no. 6, pp. 1445–1448, Jun. 2017.
[20] W. Zeng, J. Zhang, S. Chen, K. P. Peppas, and B. Ai, "Physical layer security over fluctuating two-ray fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8949–8953, Sep. 2018.
[21] G. D. Durgin, T. S. Rappaport, and D. A. de Wolf, "New analytical models and probability density functions for fading in wireless communications," *IEEE Trans. Commun.*, vol. 50, no. 6, pp. 1005–1015, Jun. 2002.
[22] M. Yacoub, "The κ-μ distribution and the η-μ distribution," *IEEE Antennas Propag. Mag.*, vol. 49, no. 1, pp. 68–81, Feb. 2007.
[23] J. M. Romero-Jerez, F. J. Lopez-Martinez, J. F. Paris, and A. J. Goldsmith, "The fluctuating two-ray fading model: Statistical characterization and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4420–4432, Jul. 2017.
[24] M. Slack, "The probability distributions of sinusoidal oscillations combined in random phase," *J. Inst. Electr. Eng. III, Radio Commun. Eng.*, vol. 93, no. 22, pp. 76–86, Mar. 1946.
[25] S. Rice, "Probability distributions for noise plus several sine waves—The problem of computation," *IEEE Trans. Commun.*, vol. COM-22, no. 6, pp. 851–853, Jun. 1974.
[26] M. Simon, "On the probability density function of the squared envelope of a sum of random phase vectors," *IEEE Trans. Commun.*, vol. COM-33, no. 9, pp. 993–996, Sep. 1985.
[27] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmWave) for 5G: Opportunities and challenges," *Wireless Netw.*, vol. 21, no. 8, pp. 2657–2676, Nov. 2015.
[28] D. Solomitckii, Q. C. Li, T. Balercia, C. R. C. M. da Silva, S. Talwar, S. Andreev, and Y. Yevgeni, "Characterizing the impact of diffuse scattering in urban millimeter-wave deployments," *IEEE Wireless Commun. Lett.*, vol. 5, no. 4, pp. 432–435, Aug. 2016.
[29] M. Di Renzo, K. Ntontin, J. Song, F. H. Danufane, X. Qian, F. Lazarakis, J. de Rosny, D.-T. Phan-Huy, O. Simeone, R. Zhang, M. Debbah, G. Lerosey, M. Fink, S. Tretyakov, and S. Shamai, "Reconfigurable intelligent surfaces vs. Relaying: Differences, similarities, and performance comparison," 2019, *arXiv:1908.08747*. [Online]. Available: http://arxiv.org/abs/1908.08747
[30] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, and I. Akyildiz, "A new wireless communication paradigm through software-controlled metasurfaces," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 162–169, Sep. 2018.
[31] E. Basar, "Transmission through large intelligent surfaces: A new frontier in wireless communications," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2019, pp. 112–117.
[32] L. Subrt and P. Pechac, "Intelligent walls as autonomous parts of smart indoor environments," *IET Commun.*, vol. 6, no. 8, pp. 1004–1010, May 2012.
[33] G. D. Durgin, "Theory of stochastic local area channel modeling for wireless communications," M.S. thesis, Virginia Polytech. Inst. State Univ., Richmond, VA, USA, 2000.
[34] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.
[35] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.
[36] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, and L. Hanzo, "Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1656–1672, Mar. 2017.
[37] G. Gomez, F. J. Martin-Vega, F. Javier Lopez-Martinez, Y. Liu, and M. Elkashlan, "Physical layer security in uplink NOMA multi-antenna systems with randomly distributed eavesdroppers," *IEEE Access*, vol. 7, pp. 70422–70435, 2019.
[38] J. Frolik, "On appropriate models for characterizing hyper-Rayleigh fading," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 5202–5207, Dec. 2008.
[39] P. C. F. Eggers, M. Angjelichinoski, and P. Popovski, "Wireless channel modeling perspectives for ultra-reliable communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 4, pp. 2229–2243, Apr. 2019.
[40] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*. 10th ed. Washington, DC, USA: U.S. Department of Commerce N.B.S, Dec. 1972.
[41] A. Abdi, H. Hashemi, and S. Nader-Esfahani, "On the PDF of the sum of random vectors," *IEEE Trans. Commun.*, vol. 48, no. 1, pp. 7–12, Jan. 2000.
[42] H. Shen, W. Xu, S. Gong, Z. He, and C. Zhao, "Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications," *IEEE Commun. Lett.*, vol. 23, no. 9, pp. 1488–1492, Sep. 2019.
[43] P. Ramirez-Espinosa and F. J. Lopez-Martinez, "Backing off from Rayleigh and Rice: Achieving perfect secrecy inwireless fading channels," in *Proc. 35th URSI Nat. Symp.*, 2020, pp. 1–4.

PABLO RAMÍREZ-ESPINOSA received the M.Sc. and Ph.D. degrees in telecommunication engineering from the University of Malaga, Spain, in 2017 and 2020, respectively. From 2017 to 2020, he was an Assistant Researcher with the Communication Engineering Department, University of Malaga. In 2018, he was a Visiting Researcher with the Queen's University of Belfast. In March 2020, he joined the Electronic Systems Department, Connectivity Section, Aalborg University, where he is currently a Postdoctoral Researcher. His main research activities are in wireless communications, particularly channel modeling and physical layer security, and applied statistics. In 2019, he received the IEEE Transactions on Communications Exemplary Reviewer Certificate.

R. JOSÉ SÁNCHEZ-ALARCÓN received the B.Sc. and M.Sc. degrees in telematics engineering from the University of Malaga, Spain, in 2018 and 2019, respectively. In 2019, he was an Assistant Researcher with the Communication Engineering Department, University of Malaga. He is currently with Datlight as a Research Engineer.

F. JAVIER LÓPEZ-MARTÍNEZ (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in telecommunication engineering from the University of Malaga, Spain, in 2005 and 2010, respectively. He was an Associate Researcher with the Communication Engineering Department, University of Malaga, from 2005 to 2012. He was a Marie Curie Postdoctoral Fellow with the Wireless Systems Lab, Stanford University, from 2012 to 2014, and with the University of Malaga, from 2014 to 2015. He was a Visiting Researcher with the University College London, in 2010, and Queen's University Belfast, in 2018. Since 2015, he has been a Faculty Member with the Communication Engineering Department, University of Malaga, where he is currently an Associate Professor. His research interests include a diverse set of topics in the wide areas of communication theory and wireless communications, including stochastic processes, wireless channel modeling, physical layer security, and wireless powered communications. He received several research awards, including the Best Paper Award from the Communication Theory Symposium at the IEEE GLOBECOM 2013, the IEEE Communications Letters Exemplary Reviewer Certificate, in 2014 and 2019, and the IEEE Transactions on Communications Exemplary Reviewer Certificate, in 2014, 2016, and 2019. He is an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS in the area of wireless communications.